CLAIMS

1. In a communications system, a method of transforming a set of message signals representing a message comprising the steps of

first encoding one of said set of message signals in accordance with a first keyed transformation;

second encoding said one of said set of message signals in accordance with at least one additional keyed transformation;

third encoding said one of said set of message signals in accordance with a self inverting transformation in which at least one of said set of message signals is altered;

fourth encoding said one of said set of message signals in accordance with at least one additional inverse keyed transformation wherein each of said at least one additional inverse keyed transformation is a corresponding inverse of said at least one additional keyed transformation; and

fifth encoding said one of said set of message signals in accordance with first inverse keyed transformation wherein said first inverse keyed transformation is the inverse of said first keyed transformation;

wherein said step of first encoding is performed in accordance with a first table and in a first direction, and wherein said step of second encoding is performed in accordance with said first table.

2. The method of claim 1, wherein said step of second encoding is performed in accordance with said first table in said first direction.

3. The method of claim 1, wherein said step of fourth encoding is performed in accordance with at least one additional direction.

4. The method of claim 1, wherein said step of fifth encoding is performed in accordance at least one additional direction.

5. The method of claim 1, wherein said first table is a permutation.

6. The method of claim 1, wherein said step of third encoding is performed in accordance with a keyed transformation.

7. The method of claim 1, wherein said step of third encoding is performed in accordance with an unkeyed transformation.

8. The method of claim 1, wherein said first keyed transformation comprises the steps of:

receiving an index value;
receiving a table; and
performing a table lookup in accordance with said index value and said table.

9. The method of claim 8, further comprising processing said index value and wherein said step of performing a table lookup is performed in accordance with the result of said processing of said index value..

10. The method of claim 9, further comprising additional processing on the result of said table lookup.

11. The method of claim 10, wherein said additional processing on the result of said table lookup comprises performing additional table lookups in accordance with said result.

12. The method of claim 10, wherein said additional processing on the result of said table lookup comprises performing Boolean operations on said result.

13. A method for mitigating a weakness in the Cellular Message Encryption Algorithm (CMEA), the method comprising:

generating a table by strict permutations; and
using the table in a substitution box of the CMEA during at least one pass of the CMEA.

14. The method of claim 13, wherein the CMEA comprises five pass encryption.

15. A method of transforming a set of message signals in a communication system, the method comprising:

generating a table by strict permutations;

first encoding one of said set of message signals in accordance with a first keyed transformation;

second encoding one of said set of message signals in accordance with a self inverting transformation in which at least one of said set of message signals is altered; and

third encoding one of said set of message signals in accordance with a second keyed transformation, wherein said second keyed transformation is the inverse of said first keyed transformation;

wherein the first and third encoding is performed in accordance with said table, and wherein the first and third encoding are performed in alternating directions.